encrypting a random session object key in a block cipher encryption process with the at least one object key;

C1
cont

encrypting a block of input plaintext data utilizing said key schedule;

modifying the at least one object key based on seeding from the random session object key;

modifying the key schedule based upon the at least one modified object key;

encrypting a next block of input plaintext data utilizing said modified key schedule; and

repeating the steps of modifying the at least one object key, modifying the key schedule and encrypting utilizing the modified key schedule until the encrypting of blocks of plaintext data is completed.

~~5~~3. (Twice Amended) A computer implemented method as defined in Claim 1, further comprising prior to the first step of encrypting the steps of:

C2

creating an initial state of the at least one object key by the user;

creating an initial state of a random session object key; and

encrypting the initial state of the random session object key in a block cipher encryption process with the initial state of the at least one object key[; and]

C2 cont

[wherein the step of modifying the at least one object key is based on seeding from the random session object key~~,~~ [before each input data block]~~,~~ so that each block of input plaintext is encrypted based on a different object key].

2/13/01 SK

2/13/01 SK TYP03

~~In Claim 21, line, please delete "2" and insert therefor --1--;~~

~~30~~ 23. (Amended) A cryptographic communications system comprising:

C3

at least two networked computer systems linked by a communication channel; and

each computer system including a central processing unit and a memory storage device for executing a block cipher encryption/decryption process;

wherein the encryption process transforms an input plaintext message to a ciphertext message and the decryption process transforms the ciphertext message to the input plaintext message, the encryption/decryption process using [a] at least one dynamic object key which [changes with] is modified using a non-linear function for each block of input data, each object key being associated with a different key schedule to encrypt/decrypt the input plaintext/output ciphertext message.

~~In Claim 34, line 3, please delete "coat" and insert therefor --count--;~~

In Claim 37, line 27, please delete "tanspositioning" and insert therefor --transpositioning--;

In Claim 37, line 29; please delete "bonded" and insert therefor --bounded--.

Please add the following new Claims 41- 43:

--~~41~~ 32. A computer implemented method for encrypting data comprising the steps of:

creating at least one object key in a block cipher, the at least one object key comprising data and methods that operate on said data;

C4

creating a key schedule based upon the at least one object key;

encrypting a block of input plaintext data utilizing said key schedule;

modifying the at least one object key using at least a non-linear function;

modifying the key schedule based upon the at least one modified object key;

encrypting a next block of input plaintext data utilizing said modified key schedule; and

repeating the steps of modifying the at least one object key, modifying the key schedule and encrypting utilizing the modified key schedule until the encrypting of blocks of plaintext data is completed.